تنفيذ توازي خط الأنابيب لنظام تشفير مبني باستخدام خوارزمية معيار التشفير المتقدم

إسراء غانم محمد
enges988@yahoo.com
Electrical Engineering Dept.

د. شفاء عبد الرحمن داؤد
shefadawwd@yahoo.com
Computer Engineering Dept.

الملخص:

في هذا البحث تم تنفيذ خوارزمية الـ AES كونها معتمدة عالمياً في تشفير المعلومات لنظم الاتصالات المختلفة أخذين بعين الاعتبار أمنيتها من الهجمات ومحاولات الاختراق وكسر الشفرة. تم في هذا البحث اقتراح منظومة تعمل على تشفير مختلف أنواع البيانات من صور وفيديو..الخ ومعاملتها معاملة النص الواحد. تم اخذ الصورة كحالة دراسة للبيانات المراد تشفيرها بالزمن الحقيقي ومن ثم إمكانية استخدام المعماريات المقترحة في تشفير البيانات الفيديوية ضمن الزمن (33 m sec) أو اقل. تم في هذه الدراسة تنفيذ معماريتين للتشفير وفك التشفير، المعمارية الأولى تمثل معمارية هجينة من نوعين مختلفين من أنواع التشفير(المتدفق والكتلي)،حيث اقترحت هذه المعمارية لغرض زيادة قوة التشفير عن طريق تقليل قوة الترابط بين النقاط الصورية، تم في هذه المعمارية تحقيق زمن مساوي لـ (16.76 µ sec) لتشفير صورة بحجم (32x64) نقطة صورية. أما المعمارية الثانية فتمثل اقتراح لخوارزمية معيار التشفير المتقدم القياسية نمط (CTR)، وتم تحقيق زمن تشفير مساوي تقريباً للزمن المحقق للمعمارية السابقة ، وبمساحة مادية مساوية لنصف المساحة تقريباً مقارنة مع المعمارية السابقة فيما لو استخدمت للتشفير أو فك التشفير وليس في آن واحد. تم تحقيق الزمن الحقيقي من خلال التنفيذ المتوازي للحسابات المطلوبة وذلك باستخدام تقنية خط الأنابيب وركبت المعماريتان المصممتان على رقاقة FPGA نوع Spartan-6 LX(XC6SLX16) باستخدام برنامج ISE 14.2 .

Pipelined Parallel Implementation of Cryptosystems Based on Advanced Encryption Standard

Abstract

A hardware architecture implementation of Advanced Encryption Standard (AES) is globally adopted to encrypt data for variant communications systems, taking into account that AES is reliable, secured and immunized against attacks. A single crypto system is suggested to encrypt and/or decrypt different types of data .These types of data are assumed to be as a text data .The image is considered as a case study for the type of data that is to be encrypted in real time. Then the proposed architectures are used to encrypt the video within the time ≤ 33 m sec . Two architectures are proposed . The first one is a hybrid of both stream and block ciphering. This architecture is used to increase the encryption security by reducing the correlation among image pixels. The resulting encryption time for an image of (32x64) pixels is equal to 16.76 µ sec. The second architecture is proposed for CTR mode of AES algorithm. The same time achieved in the first architecture is also achieved in this implementation. However ,the half of the hardware resources in comparison with the first architecture is achieved in implementing the second, but if it is used for either encryption or decryption , not for both simultaneity. The real time implementation is achieved due to using parallel computation that is based on pipelining technique. The architecture are synthesized on Spartan-6 LX(XC6SLX16) using ISE 14.2 .

Keywords : AES , FPGA , Image Encryption , Pipeline design .

أستلم: 17 – 11 - 2013 قبل: 6 – 3 - 2014

1- المقدمة :-

يجب أن تتمتع معظم البيانات التي يتم تداولها عبر وسائل الاتصال الحديث بخصوصية عالية للمستخدم والتي يمكن أن تتحقق بطرائق متعددة تعتمد على تقنيات معينة، يسمى العلم الذي يدرس هذه الطرائق وآلية عملها على البيانات المراد تشفيرها بـ "علم التشـفير". تختلف هذه الطرائق باختلاف نوع البيانات المستخدمة، وبالتالي فأن ذلك يتطلب بناء منظومة للتشفير وفك التشفير لكل نوع من أنواع البيانات [1]. على الرغم من اختلاف الطرائق والمفاهيم المترتبة عليها ألا إن جميعها يشترك في الهدف نفسه وهو تحويل البيانات التي يمكن لأي شخص فهمها إلى بيانات مُبهمة يصعب على الأشخاص غير المُخولين فهمها وذلك من خلال تطبيق وظائف حسابية ومجموعة ثابتة من الخطوات عليها لأجراء ذلك التحويل. يمكن تطبيق طرائق التشفير على مختـلف أنواع البيانات من نصوص، صور، صوت وفيديو ... الـخ . غـالبية هذه البيانات تحتاج إلى تنفيذ في الزمن الحقيقي لمواكبة تطور الأجهزة الحديثة. تستخدم تقنية مصفوفة البوابات القابلة للبرمجة حقلياً في تنفيذ المنظومات وذلك لخاصيتها في إمكانية إعادة برمجتها تبعاً لحاجة المستخدم، ألا إن تخصيص نوع مختلف من المنظومات مع اختلاف البيانات يؤدي إلى زيادة كلفة المنظومة وتعقيدها فيما لو طبقت مادياً، تم في هذا البحث تصميم وتنفيذ منظومة تشفير وفك التشفير تعامل البيانات المختلفة معاملة النص الواحد. تم اعتماد خوارزمية معيار التشفير المتقدم AES بأنماط معينة اعتماداً على قابلية تنفيذ الحسابات بشكل متوازي لتشفير مختلف بيانات الوسائط المتعددة ومعاملتها معاملة النص. لتنفيذ هذه الأنماط وتحقيق متطلبات الزمن الحقيقي (30 Frame/Sec) فأن ذلك يتطلب تصميم ذو كفاءة عالية . يمكن تحقيق ذلك باستخدام تقنية خط الأنابيب وذلك لتقليص زمن عملية المعالجة لأنماط التشفير تبعاً لهيكلية كل نمط. من الجدير بالذكر أن بعض التطبيقات تحتاج إلى تنفيذ تصاميم تعمل على التشفير وفك التشفير في آن واحد كما هو الحال في الهواتف النقالة ، أما الأنظمة التي تحتاج إلى التشفير فقط فيمكن ان تطبق في الكاميرات الرقمية. منذ اعتماد خوارزمية معيار التشفير المتقدم من قبل المعهد الوطني للمعايير والتكنولوجيا (NIST)، توالت البحوث في استخدام الخوارزمية في تشفير مختلف أنواع البيانات، وفيما يلي بعض الأعمال التي تم العمل بها في السنوات السابقة، ففي عام 2002 قام كل من الباحثين Xinmiao.Z وK. Parhi بدراسة عدة أساليب لتنفيذ خوارزمية معيار التشفير المتقدم، وذلك بالاعتماد على الوفرة في كمية الموارد المتاحة إضافة إلى السرعة المطلوبة أثناء عملية المعالجة [2]، وفي عام 2005 قام S.Yooوآخرون بتنفيذ خوارزمية معيار التشفير المتقدم والعمل على تحسين أدائها وذلك باستخدام تقنية خط الأنابيب. كان الهدف من البحث تحقيق سرعة عالية من خلال الاستخدام المتوازي والمتمثل بتقنية خط الأنابيب [3]، وفي عام 2009 قامت الباحثة F.Shamsulddin بتنفيذ خوارزمية معيار التشفير المتقدم واقتراح طريقة لتشفير الصور، كان الهدف من البحث تقليل قوة الترابط بين العناصر المتجاورة والموجودة في غالبية الصور، تلخصت فكرة البحث ببـعثرة عناصر الصورة وذلك باستخدام مولد تسلسل شبه عشوائي[4] ، وفي عام 2012 قام S. Saha وآخرون بتنفيذ خوارزمية معيار التشفير المتقدم، حيث كان الهدف من البحث تحقيق اتصال امن بين حاسبتين مع وجود رقاقتين FPGA وذلك خلال الزمن الحقيقي [5] . في عام 2013 قام كل من الباحثين Muhaya و F. Bin باقتراح طريقة لتشفير صور الأقمار الصناعية، تم في ذلك البحث تشفير الصور الهامة والسرية باستخدام نوعين من التشفير، يُمثل الأول التشفير الفوضوي والذي بدوره يستخدم خارطة Arnold's cat لأجل تشويش قيم النقاط الصورية، أما النوع الثاني من التشفير فيستخدم خوارزمية معيار التشفير المتقدم للتشفير بشكل كتل للبيانات الصورية المشفرة التي تم الحصول عليها من النوع السابق من التشفير [6].

2- أنواع التشفير

يقسم التشفير بشكل عام إلى نوعين [7]:

1.2 تشفير المفتاح المتناظر

وفيه يكون مفتاح التشفير وفك التشفير متماثلان هذا النوع قد يتطلب قناة إضافية آمنة تعمل على نقل المفتاح المتناظر بين الطرفين. يقسم التشفير المتناظر بدوره إلى نوعين، النوع الأول يقوم بتشفير البيانات على مستوى البايت الواحد وبذلك يمكن استثماره في بعض التطبيقات التي تحتاج تشفير كل بايت أصلي يتم إدخاله ويسمى بالتشفير المتدفق. أما النوع الثاني فيقوم بعملية التشفير على مجموعة من البايتات وذلك بتقسيم البيانات الداخلة إلى مجموعة من الكتل وبالتالي فأنه يقوم بتشفير كل كتلة على حدا، يتسم هذا النوع بأنه اقل سرعة من التشفير المتدفق .

2.2 تشفير المفتاح غير المتناظر

ويكون فيه مفتاح التشفير وفك التشفير غير متماثلان وهو بذلك لا يحتاج إلى قناة إضافية لنقل المفتاح يحتوي هذا النوع على مفتاحين، الأول يكون عام ويكون معروف للعامة ويسمى المفتاح العام (Public Key) ، أما المفتاح الثاني فيكون سري لا يعرفه سوى الشخص المخول ويسمى بالمفتاح الخاص (Private Key) .

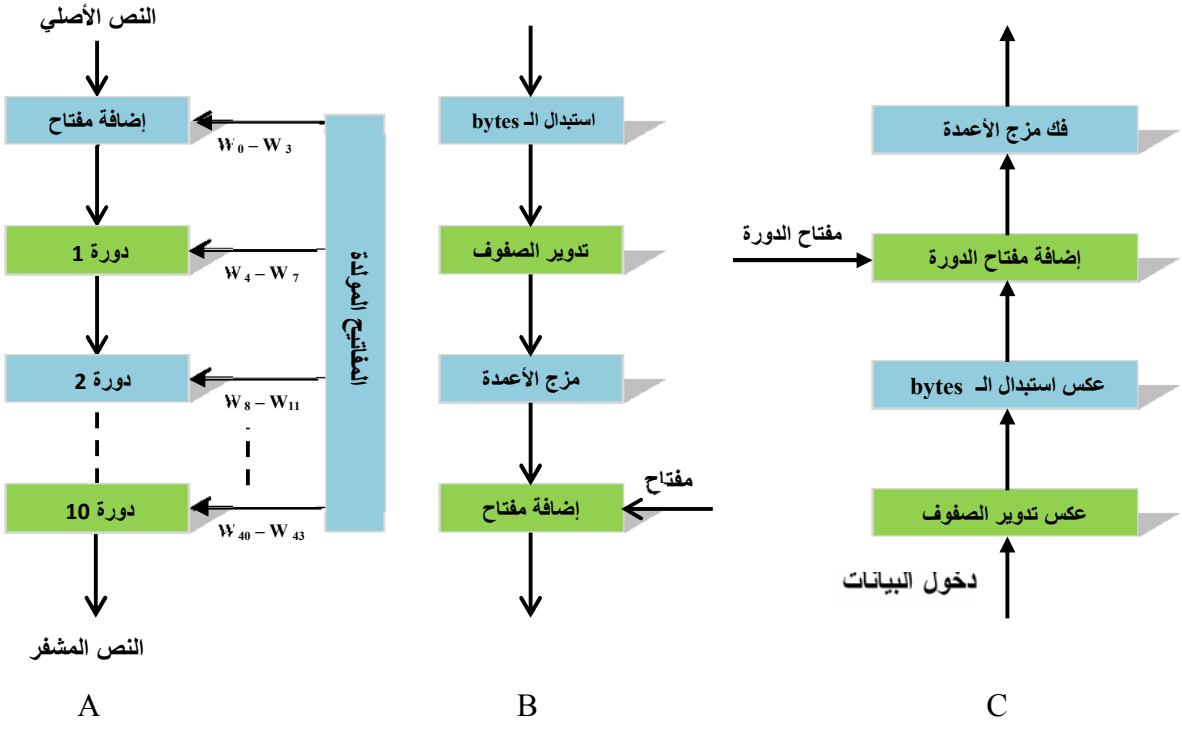
3- هيكلية خوارزمية معيار التشفير المتقدم- ريجندال (AES-Rijindal)

تم تطوير خوارزمية معيار التشفير المتقدم في عام 1997 من قبل الباحثين John Daemen و Vincent Rijmen والتي تم اعتمادها فيما بعد من قبل المعهد الوطني للمعيار والتكنولوجيا على أنها معياراً للتشفير المتقدم [8]. يمكن وصف هيكلية خوارزمية الـ AES على أنها مجموعة من الدورات المتتابعة كل دورة تحوي على مجموعة من المراحل .

تصنف خوارزمية معيار تشفير المتقدم على أنها خوارزمية تشفير مفتاح متناظر تقوم بتشفير البيانات بشكل كتل، تُتيح هذه الخوارزمية إمكانية إدخال كتل ومن ثم تشفيرها بأحجام مختلفة من المفاتيح حسب حاجة المستخدم، وعلى هذا الأساس يمكن تقسيم الخوارزمية إلى ثلاث أقسام ثابتة بحسب حجم المفتاح الذي يتم التشفير من خلاله وكما يلي [9] .

- خوارزمية معيار التشفير المتقدم حجم المفتاح يساوي 128 بت ، تتطلب 10 دورات لإكمال التشفير أو فك التشفير.
- خوارزمية معيار التشفير المتقدم حجم المفتاح يساوي 192 بت ، تتطلب 12 دورة لإكمال التشفير أو فك التشفير.
- خوارزمية معيار التشفير المتقدم حجم المفتاح يساوي 256 بت ، تتطلب 14 دورة لإكمال التشفير أو فك التشفير.

في هذا البحث سيتم اخذ النوع الأول كحالة دراسة. والذي يتكون كما تم ذكره من 10 دورات، كل دورة تتكون من أربع مراحل عدا الدورة الأخيرة فأنها مكونة من ثلاث مراحل فقط ، هذه المراحل تختلف في تسلسلها وآلية عملها في حالة التشفير عما هو عليه في حالة فك التشفير كما موضح في الشكل (1) .



الشكل (1) : A) دورات التشفير في خوارزمية AES ، B) مراحل الدورة الواحدة في عملية التشفير C) مراحل الدورة الواحدة في عملية فك التشفير

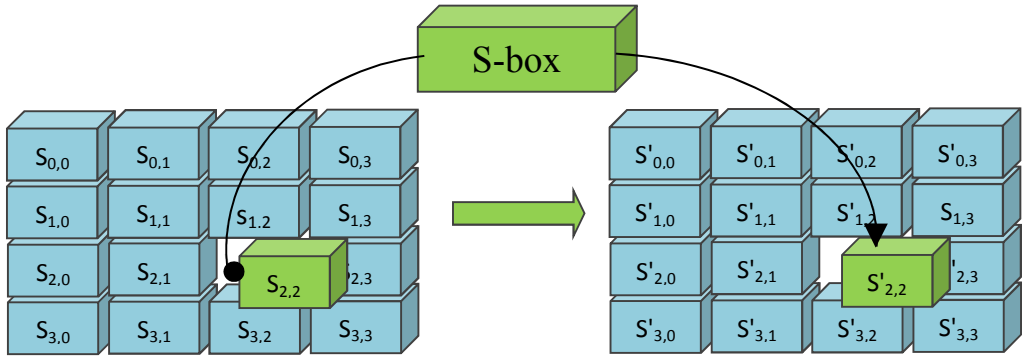
كما يمكن تصنيف هذه الخوارزمية إلى خمس أنماط تختلف في طريقة إدخال النص الأصلي المراد تشفيره وكما يلي.

1. نمط جدول الترميز الالكتروني (The Electronic Codebook Mode - ECB)
2. نمط سلسلة الكتل المشفرة (The Cipher Block Chaining Mode - CBC)
3. نمط التغذية الخلفية بالنص المشفر (The Cipher Feedback Mode – CFB)
4. نمط التغذية الخلفية بالإخراج (The Output Feedback Mode -OFB)
5. نمط العداد (The Counter Mode - CTR)

1.3 مراحل تشفير الدورة الواحدة

1) مرحلة الاستبدال

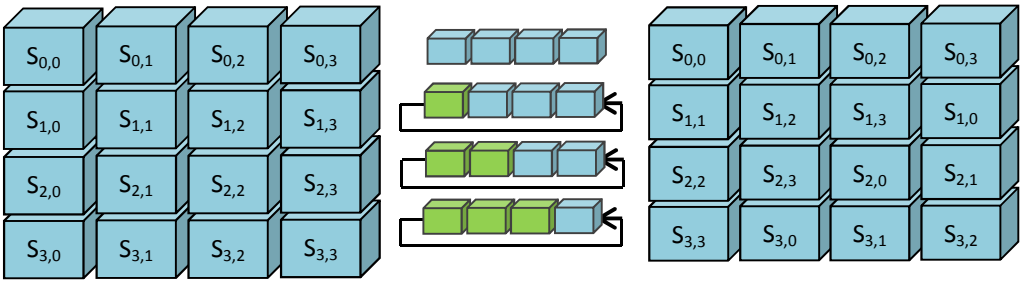
في هذه المرحلة يتم استبدال كل بايت يتم استقباله بقيمه أخرى كما موضح في الشكل(2)، وذلك بأخذ القيمة المراد استبدالها وتقسيمها إلى جزئين، الجزء الأول MSB يمثل الصف في مصفوفة صندوق الاستبدال (S-box)، أما الجزء الثاني LSB فيمثل العمود، بتقاطع الصف والعمود تظهر لنا قيمة والتي تمثل ناتج عملية الاستبـدال .



الشكل (2) : عملية الاستبدال

2) مرحلة تدوير الصفوف

في هذه المرحلة يتم استلام الكتلة والتي تكون على شكل مصفوفة مربعة 16 بايت S[i, j] بأبعاد (4×4) كما في الشكل (3) ، يتم إبقاء الصف الأول بدون تدوير، أما الصف الثاني فيتم تدويرهُ مرتبة واحدة (1 بايت) نحو اليسار وهكذا يتم تدوير باقي الصفوف بمقدار 2 , 3 byte على التوالي .



الشكل (3) : عملية التدوير

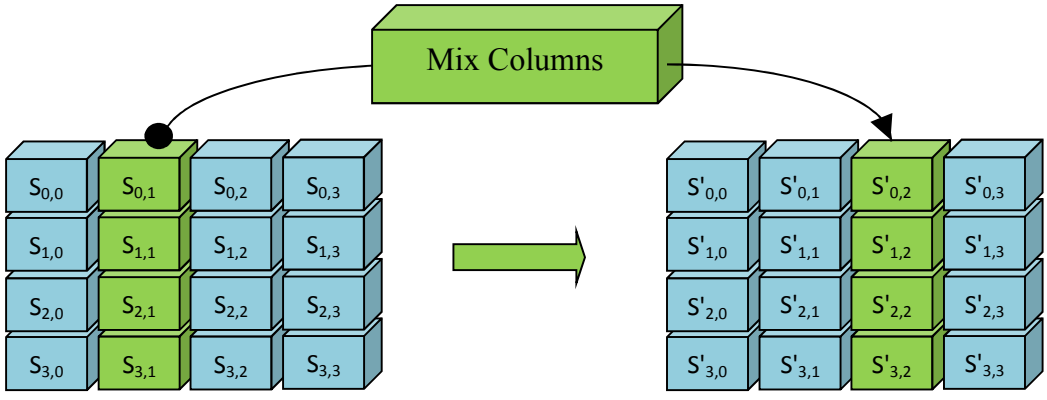
3) مرحلة مزج الأعمدة

في هذه المرحلة يتم استبدال كل بايت في المصفوفة S[i, j] بقيم أخرى تعتمد على قيم العناصر التابعة لنفس العمود لتنتج بذلك مصفوفة S′[i, j] ،كما موضح في الشكل (4) ،وهي بذلك تعتبر أول مرحلة تأخذ بنظر الاعتبار قيم العناصر المجاورة أثناء عملية المعالجة وفق المعادله (1)، توجد هذه المرحلة في جميع الدورات عدا الدورة الأخيرة.

$$
\begin{aligned}
s'_{0,j} &= (2 \bullet s_{0,j}) \oplus (3 \bullet s_{1,j}) \oplus s_{2,j} \square s_{3,j} \\
s'_{1,j} &= s_{0,j} \square (2 \bullet s_{1,j}) \oplus (3 \bullet s_{2,j}) \oplus s_{3,j} \\
s'_{2,j} &= s_{0,j} \square s_{1,j} \square (2 \bullet s_{2,j}) \oplus (3 \bullet s_{3,j}) \\
s'_{3,j} &= (3 \bullet s_{0,j}) \oplus s_{1,j} \square s_{2,j} \square (2 \bullet s_{3,j})
\end{aligned}
\qquad \ldots\ldots (1)
$$

حيث ان :

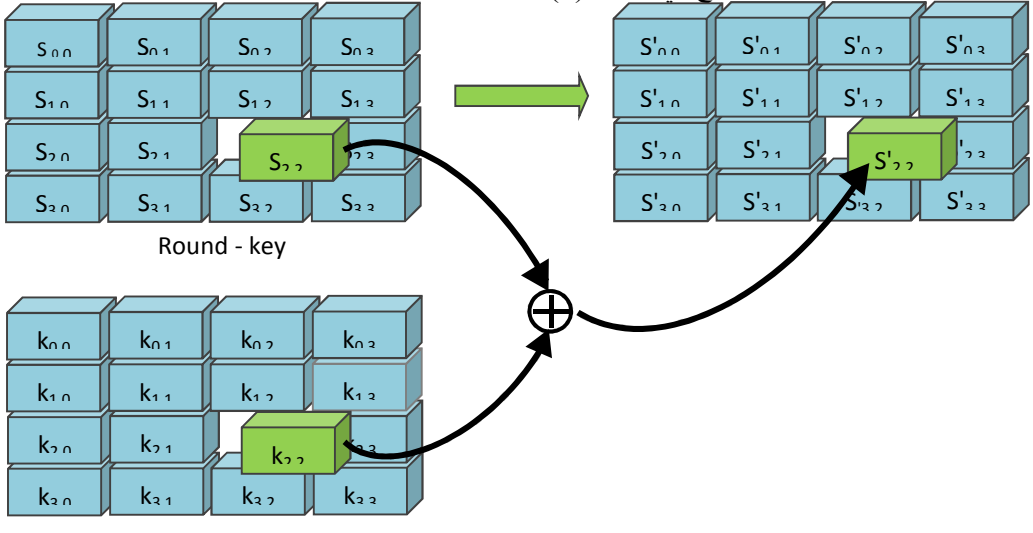
- $\square$: تمثل عملية XOR
- $\bullet$: عملية ضرب باستخدام المجال المحدد $GF(2^8)$ (Galois field)



الشكل (4) : مرحلة مزج الأعمدة

4) مرحلة إضافة مفتاح الدورة

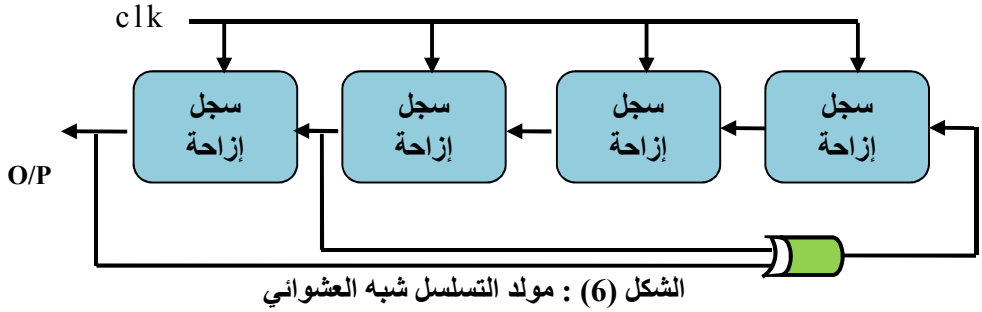
يتم في هذه المرحلة إضافة المفتاح الذي تم توليده وذلك باستخدام عملية XOR لربط المفتاح مع الناتج الذي تم إيجاده من العملية السابقة ، كما موضح في الشكل (5) .



الشكل (5) : عملية إضافة المفتاح

4- مولد التسلسل شبه العشوائي (Pseudo Random Sequence Generator - PRSG)

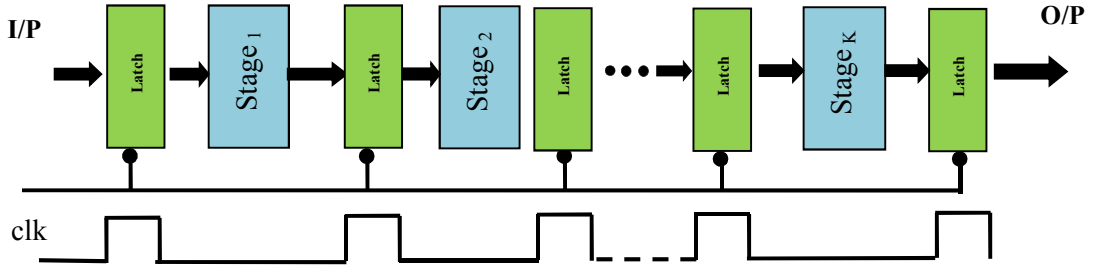
يبنى عمل هذا المولد على أساس وجود مجموعة من السجلات كما موضح في الشكل (6) . عدد الاحتمالات التي يمكن أن تُولد تعتمد على عدد هذه السجلات، حيث ان عدد الاحتمالات التي يمكن ان تولد تساوي $2^n - 1$ ، حيث n تمثل عدد السجلات ، يستخدم هذا المولد في تطبيقات عديدة منها توليد مفاتيح لتشفير البيانات وكذلك في التطبيقات التي تحتاج إلى اخذ عينات عشوائية لمجموعة كبيرة من البيانات [10] [11] .



الشكل (6) : مولد التسلسل شبه العشوائي

5- تقنية خط الأنابيب (Pipeline) :-

تعتبر تقنية خط الأنابيب إحدى أهم التقنيات المتوازية والمستخدمة لتسريع النظم. تنبني هذه التقنية على أساس وجود مجموعة من المراحل (Stages-S) المتتالية كما موضح في الشكل (7)، يتم وضع مزلاج (Latch) بين مرحلة وأخرى يعمل على حفظ بيانات المرحلة السابقة وذلك لكي يتسنى الوقت للبيانات الداخلة الجديدة العمل عليها. من الشكل(7) يمكن ملاحظة ان التقنية تعتمد على نابض (Clock) مشترك والذي يعمل على السيطرة على سير البيانات على طول مسار التقنية. توفر تقنية خط الأنابيب إمكانية تحقيق سرعة عالية لأداء النظام وذلك من خلال إمكانية إتاحة العمل بشكل متوازي على الرغم من تركيبها المتوالي بحيث ان البيانات الداخلة لا تنتظر لحين خروج الإدخال السابق لكي يتم إدخالها، وهذا مايجعلها من أهم التقنيات المستخدمة في المعالجة المتوازية للوسائط المتعددة [12] . تعمل هذه التقنية بكفاءة عندما يتكون الإدخال من عدد كبير من المهام المتتالية .



الشكل (7) مراحل تقنية خط الأنابيب

6- أساليب تنفيذ المعماريات المصممة

1. الأسلوب الحلقي: يتم في هذا الأسلوب تنفيذ معماريتي التشفير وفك التشفير بشكل حلقي ، وذلك من خلال استغلال الميزة التي تتيحها كلا المعماريتين، وهي ان معظم الدورات تشترك في التصميم ذاته وذلك من خلال تنفيذها لعمليات حسابية متشابهه، وهذا يتيح إمكانية تصميم المعمارية بأكملها بالاعتماد على تنفيذ دورة واحدة فقط [2].

2. أسلوب خط الأنابيب: في هذا الأسلوب يتم تنفيذ المعمارية بالاعتماد على تقنية خط الأنابيب، وذلك باعتبار كل دورة من دورات الـ AES عبارة عن مرحلة من مراحل تقنية خط الأنابيب [2].

3. أسلوب خط الأنابيب المجزئ: يتم تنفيذ المعمارية في هذا الأسلوب بالاعتماد على تقنية خط الأنابيب أيضا، ولكن على اعتبار ان كل مرحلة من مراحل التشفير أو فك التشفير تمثل مرحلة من مراحل تقنية خط الأنابيب مع إمكانية تجزئة الدورة إلى مراحل جزئية [2].

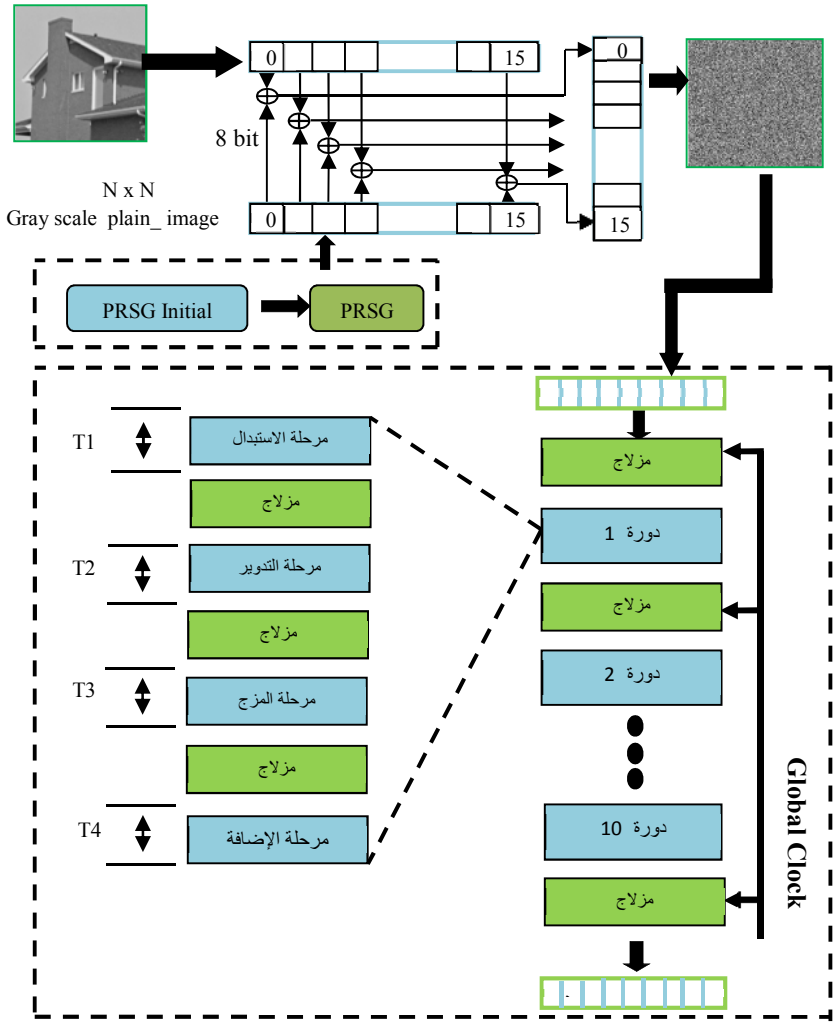
7- المعماريات المصممة

لبيان كفاءة الخوارزميتين المقترحتين في الزمن الحقيقي سيتم اخذ الصورة والفيديو كحالة دراسة. تتكون الصورة من عدد هائل من النقاط الصورية وبالتالي يجب استخدام تقنيات معينة لها القابلية على التعامل مع هذا الكم الهائل من البيانات المتدفقة، لذلك فقد تم اعتماد تقنية خط الأنابيب لكفاءتها في معالجة البيانات المكونة من عدد كبير من المهام المتتالية كما تم ذكره في القسم (5). بالإضافة إلى حجم البيانات الكبير فأن الصور تمتاز بوجود نسبة ترابط كبيره بين النقاط الصورية المتجاورة المكونة لها، وبالتالي فأن من الضروري فك الترابط الموجود لزيادة قوة التشفير. يتم حل هذه المشكلة باستخدام مولد تسلسل شبه عشوائي (PRSG) والذي يتم إضافته إلى المعمارية المصممة بطريقة معينة سيتم ذكرها لاحقاً. يتم في هذا البحث تنفيذ نمط الـ ECB ونمط الـ CTR المقترحين، وذلك عن طريق تجزئة الصور المراد تشفيرها إلى كتل كل كتلة مكونة من 128 بت وهو ما يتلاءم مع حجم كتل خوارزمية الـ AES . يمكن تنفيذ نمط الـ (ECB) و(CTR) بشكل متوازي وذلك لعدم اعتماد معالجة(تشفير) الكتلة الحالية على ناتج الكتلة السابقة.

1.7 المعمارية المقترحة الأولى

في هذا المقترح يتم إدخال بيانات الصورة إلى الخوارزمية المقترحة كما موضح في الشكل (8)، بعد دخول البيانات يتم دمجها بعملية XOR مع الاحتمالات المولدة بواسطة مولد التسلسل شبه العشوائي وبالتالي يتم التخلص من المشكلة الأولى التي يتميز بها هذا النوع من البيانات (الترابط بين النقاط الصورية) بعد ذلك يتم إدخال كل ناتج من العملية

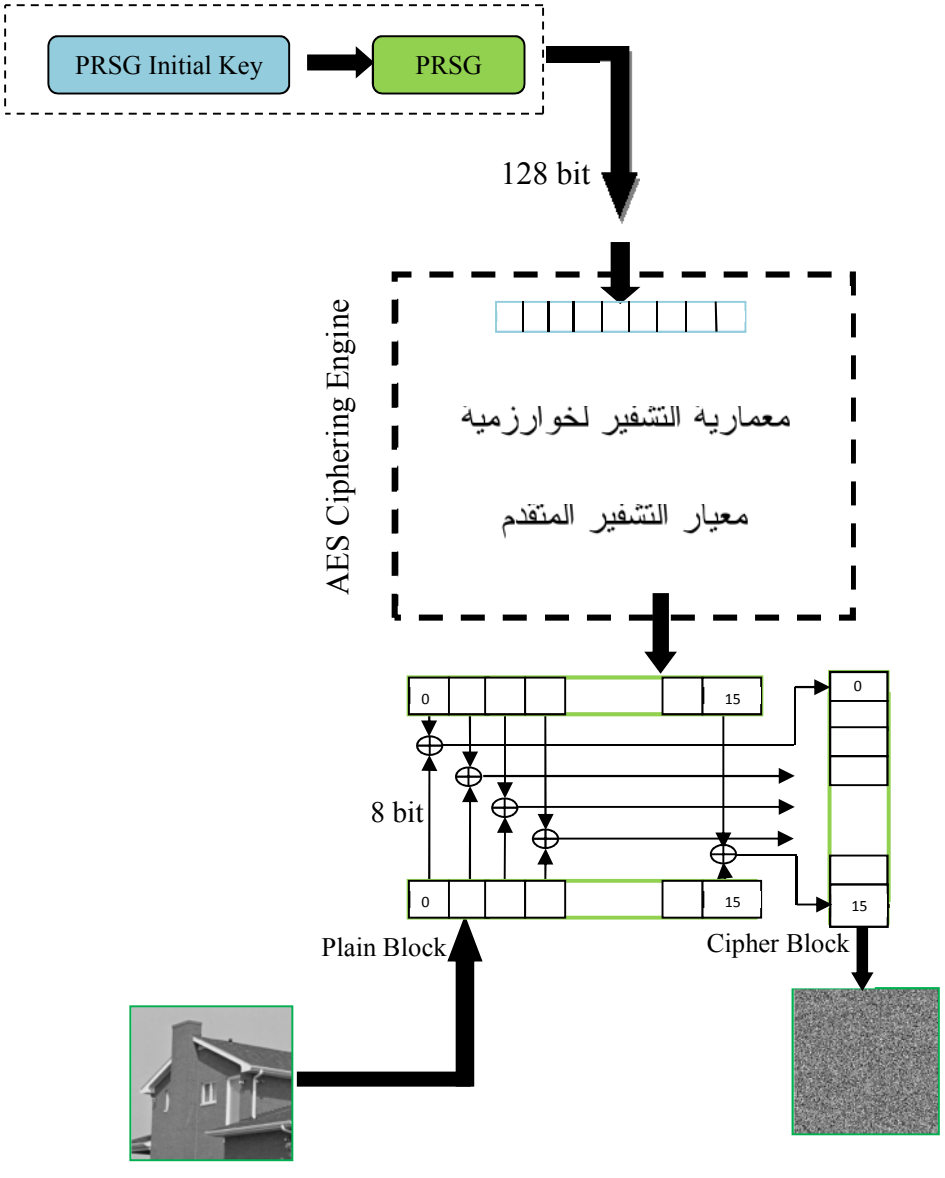
السابقة وبشكل أني إلى خوارزمية الـ AES وذلك باستخدام تقنية خط الأنابيب لتقليل الزمن اللازم لعملية المعالجة وتحقيق الزمن الحقيقي. في نفس الوقت فأن كل كتلة يتم تشفيرها يتم إعادة ترتيبها بنفس التسلسل الذي كانت عليه لتكوين الصورة المشفرة .أما في حالة فك التشفير فان الصورة المشفرة يتم إدخالها إلى معمارية فك التشفير مع ملاحظة أن الدمج الذي يتم مع مولد التسلسل شبه العشوائي يتم بعد خوارزمية فك التشفير للـ AES .



الشكل (8) : آلية عمل المعمارية المقترحة الأولى

2.7 المعمارية المقترحة الثانية

في هذه المعمارية يتم استخدام نمط الـ CTR، يتيح هذا النمط أمكانية التنفيذ بشكل متوازي أيضاً وبالتالي إمكانية استخدام تقنية خط الأنابيب. يتم في هذا النمط استخدام خوارزمية التشفير في عملية فك التشفير، تقوم خوارزمية الـ AES في هذا النمط بتشفير العداد الذي يتم إدخاله إلى الخوارزمية، وليس النص الأصلي (الصورة) كما في المعمارية السابقة [13]، بعد إجراء عملية التشفير للعداد يتم دمج الكتلة المشفرة بالنص الأصلي بعملية XOR . يتم اختيار العداد لكي يقوم بإعطاء قيم مختلفة في كل حالة، في المعمارية المقترحة يتم استبدال العداد لكي يقوم بإعطاء قيمه عشوائية في كل حالة وذلك لغرض زيادة قوة التشفير كما موضح في الشكل (9) مع ضرورة عدم تكرار الاحتمالات المولدة وذلك لزيادة قوة التشفير .

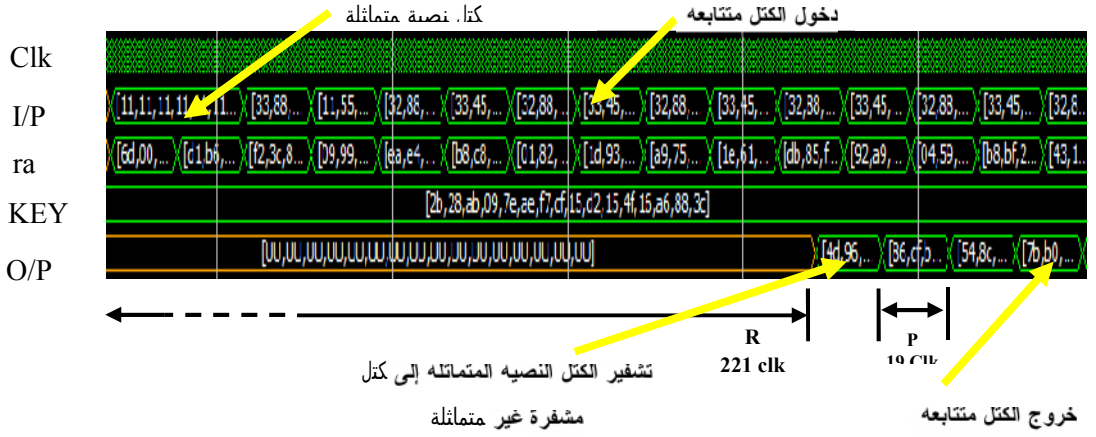


الشكل (9) : آلية عمل معمارية التشفير وفك التشفير المقترحة الثانية

8- النتائج

1.8 نتائج التنفيذ المادي

تم تنفيذ المعماريتين المقترحتين على رقاقة Spartan 6 (xc6slx16) باستخدام برنامج ISE 14.2. من الشكل (10) يمكن ملاحظة النتائج التي تم الحصول عليها من خلال المخطط الزمني الموضح فيه استخدام تقنية خط الأنابيب والتي تظهر فيه الكتل المشفرة تباعاً وذلك بعد تدفق المهام بشكل متتابع. أما كمية الموارد التي تم استخدامها فإنها تتيح إمكانية تركيب التصاميم على الشريحة المذكورة والتي يمكن إدراجها في الجدول (1) .



الشكل (10) : نتائج المحاكاة للمعماريتين المقترحة الأولى و الثانية .

جدول (1) : يوضح كمية الموارد المستخدمة لبناء المعماريتين

Device Utilization Summary (estimated values)					
Logic Utilization	Used/ENC1/ ENC2/DEC2	Used/ DEC1	Available	Utilization/ENC1 / ENC2/DEC2	Utilization/ DEC1
Number of Slice Registers	6874	10,946	18224	37%	60%
Number of Slice LUTs	5307	6,904	9112	58%	75%
Number of fully used LUT-FFpairs	3308	5,669	8873	37%	65%
Number of Block RAM/FIFO	1	1	32	3%	3%
Maximum Frequency	158.234 MHz				

2.8 نتائج التنفيذ البرمجي

في هذا القسم يتم توضيح للنتائج التي تم الحصول عليها من خلال التنفيذ البرمجي للمعماريات المنفذة مادياً، وذلك باستخدام صورة رمادية النوع لغرض إجراء عملية المعالجة عليها والتي تمت من خلال استخدام m-file في برنامج Matlab . في الشكل (11) يمكن ملاحظة الصورة الأصلية والصور المشفرة بالمعماريتين المقترحتين .

C B A

الشكل (11) : A– يمثل الصورة الأصلية , B - صورة مشفرة بواسطة المعمارية المقترحة الأولى , C – صورة مشفرة بواسطة المعمارية المقترحة الثانية

1.2.8 نتائج التحليل الإحصائي

1 - نتائج قوة الترابط والانتروبي للمعماريات المصممة

يتم في هذا القسم استعراض مجموعة من النتائج التي تم الحصول عليها من تنفيذ المعماريات المصممة والتي تمثل اختبارات قوة التشفير للصور التي تم معالجتها، والتي يمكن إدراجها في الجدول (2). يلاحظ من خلال الجدول عامل الترابط بين نقاط الصورة بالمستوى الأفقي والعمودي إضافة إلى حساب الانتروبي لكل صورة تم استخدامها، كما يمكن ملاحظة التحسن في عامل الترابط من خلال تقليل الترابط بين النقاط الصورية وذلك عند استخدام مولد التسلسل شبه

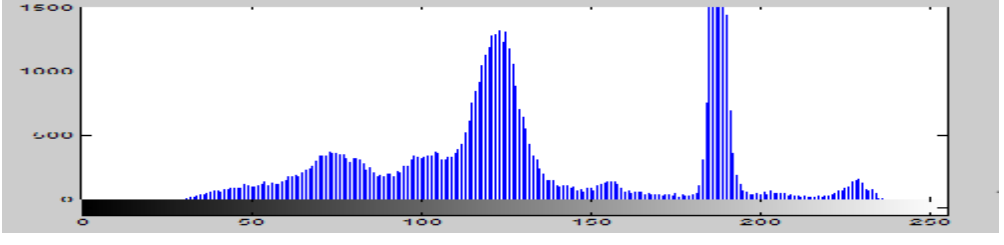
العشوائي، بالإضافة إلى ملاحظة التحسن (زيادة) الانتروبي والتي تعتبر مقياس للعشوائية، حيث تكون الانتروبي مساوية للصفر عندما تكون الصورة مكونة من تدرج رمادي واحد وأعلى ما يمكن عندما تكون عشوائية بالكامل .

الجدول(2) : قياس قوة الترابط والانتروبي .

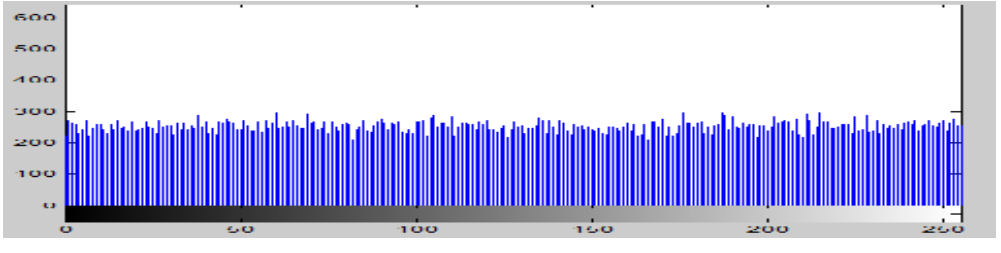
Image	Correlation Analysis		Entropy value
	Vertical	Horizontal	
الصورة الأصلية	0.96528	0.97807	6.4971
ECB	0.0072677	0.00056767	7.9971
المقترحة 1	0.0026851	-0.00074783	7.9969
CTR	0.00023802	-0.0023204	7.9969
المقترحة 2	-0.00018942	0.0019987	7.9974

2نتائج المدرج التكراري (Histogram) للمعماريات المصممة

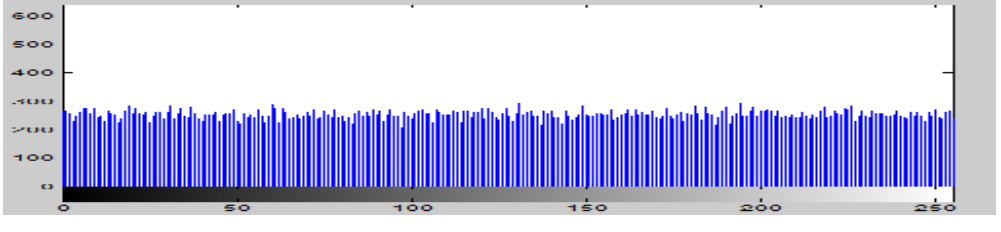
في هذا القسم يتم إدراج مجموعة من الأشكال والتي تمثل المدرج التكراري للصورة التي تم أخذها كحالة دراسة بحيث يمكن ملاحظة النتائج بوضوح في الشكل (12) ، وذلك من خلال المقارنة بين الأشكال من ناحية انتظامها، ففي حال استخدام معماريات التشفير المقترحة فان الأشكال تكون منتظمة مقارنة مع الصورة الأصلية .



الصورة الأصلية



صورة مشفرة بواسطة المعمارية المقترحة الأولى



صورة مشفرة بواسطة المعمارية المقترحة الثانية

الشكل (12) : المدرج التكراري لمجموعة من الصور

9- قياس الأداء

يمكن حساب الزمن المستغرق لتشفير صورة بحجم (32 x 64) لكلا المعماريتين وذلك باستخدام المعادلة (2) .

$$\text{Time of Pipeline(Image)} = \frac{C}{F} = \frac{((B-1) \times P) + R}{F} \quad \ldots\ldots (2)$$

B : عدد الكتل التي يتم معالجتها وتساوي 128.
P : عدد النبضات خلال كل إخراج وتساوي 19 .
R : عدد النبضات اللازمة لتشفير الكتلة الأولى وتساوي 221 .
F : التردد المستخدم ويساوي 158.234 MHz .

$$Time\ of\ Pipeline(Image) = \{ [(((32*64) / 16) -1) *19] +221\} /158.234 \text{ MHz}$$
$$= 16.64\ \mu s$$

أما التسارع ($Speedup$) فيمكن حسابه وفق المعادلة (3) .

$$Speedup = \frac{Time\ of\ Non-Pipeline}{Time\ of\ Pipeline} \quad \ldots\ldots (3)$$

$$\therefore Time\ of\ Non-Pipeline = \frac{B*R}{F} \quad \ldots\ldots (4)$$

$$Time\ of\ Non-Pipeline(Image) = \frac{128 \times 221}{158.234} = 178.77\ \mu sec$$

$$\therefore Speedup = \frac{178.77}{16.64} = 10.74$$

من الملاحظ ان كلا المعماريتين تم تنفيذها وفق متطلبات الزمن الحقيقي وان الزمن المستغرق اقل بكثير من الزمن اللازم لمعالجة الفيديو($\leq 33ms$) لذلك بالإمكان تطبيق كلا المعماريتين على الصور الفديوية .

10- الاستنتاجات

في هذا البحث تم اقتراح المعماريتين وذلك لغرض زيادة قوة التشفير بالمقارنة مع المعماريتين القياسيتين (ECB , CTR)، أما من ناحية الموارد المستهلكة فتم استنتاج ان المعمارية الأولى تستخدم خوارزميتين مختلفتين تماماً تستخدم الأولى للتشفير والأخرى لفك التشفير وبالتالي فأنها تطلب تركيب الخوارزميتين على الشريحة لغرض جعل الشريحة قابلة على التشفير وفك التشفير، أما في حالة المعمارية المقترحة الثانية فأنها تتيح استخدام خوارزمية التشفير في فك التشفير وبالتالي إمكانية تركيب خوارزمية التشفير على الشريحة والتي ستقوم بدورها بالتشفير وفكه ولكن ليس في آن واحد وبالتالي اختصار الموارد اللازمة للتنفيذ. أما بالنسبة للتنفيذ في الزمن الحقيقي فأن كلا المعماريتين تم تنفيذهما ضمن متطلبات الزمن الحقيقي .

المصادر:

[1] S. Lian, "Multimedia Content Encryption" , © by Taylor & Francis Group, LLC, International Standard Book Number-13: 978-1-4200-6527-5 (Hardcover) , 2009 .

[2] X. Zhang, k. Parhi," Implementation approaches for the advanced encryption standard algorithm ", Journal: IEEE Circuits and Systems Magazine ISSN: 1531636x , 2002 .

[3] S. Yoo, D. Kotturi, W.Pan, J. Blizzard, " An AES crypto chip using a high-speed parallel pipelined architecture ", Microprocessors and Microsystems 29.7 : 317-326. , 2005.

[4] F.Shamsulddin, "On the security of Bitmap Images using Scrambling based Encryption Method" , Journal of Engineering and Development, Vol. 13, No. 3,September, ISSN 1813-7822 2009 .

[5] R. Paul, S. Saha, S. Sau, A. Chakrabarti, "Design and implementation of real time AES-128 on real time operating system for multiple FPGA communication", arXiv preprint arXiv:1205.2153, 2012 ..

[6] F. Bin , Muhay, "Chaotic and AES cryptosystem for satellite imagery ", Journal: Telecommunication Systems ISSN: 10184864**,** Volume:52 Issue:2 Pages:573-581 Provider: Springer , DOI:10.1007/s11235-011-9462, 2013 .

[7] A.Mathur,"A Research paper: An ASCII value base data encryption algorithm and its comparison with other symmetric data encryption algorithms", International Journal 4 on Computer Science and Engineering (IJCSE), 2012 .

[8] J. Daemen, V.Rijmen, "The Design of Rijndael : AES - The Advanced Encryption Standard", copyright © ISBN 3-540-42580-2 Springer-Verlag Berlin Heidelberg New York .

[9] A. Deshpande, M. Deshpande, D. Kayatanavar," FPGA Implementation of AES Encryption and Decryption" , Control, Automation, Communication and Energy Conservation, INCACEC 2009. International Conference on. IEEE, 2009 .

[10] "Efficient Shift Registers, LFSR Counters ,and Long Pseudo-Random Sequence Generators", URL: http://www.xilinx.Com/bvdocs/appnotes/xapp052 , XAPP 052 July 7,1996 (Version 1.1) .

[11] A. Kumar, P. Rajput ,et al ," Design Of Multi Bit LFSR PNRG And Performance Comparison On FPGA Using VHDL", International Journal of Advances in Engineering & Technology, March 2012. ISSN: 2231-1963 .

[12] K.Hwang , "Advanced Computer Architecture ",ISBN 0-07-031622-8, Copyright © by McGraw-Hill, Inc, 1993 .

[13] M. Dworkin, "Recommendation for Block Cipher Modes of Operation", No. NIST-SP-800-38A. National Inst of Standards and Technology Gaithersburg MD Computer Security DIV, 2001.

تم اجراء البحث في كلية ألهندسة = جامعة ألموصل